

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**  
**(Docket No. 138065UL (MHM 15115US01))**

In the Application of:

Mathew

Serial No.: 10/681,634

Filed: October 8, 2003

For: BIOMETRICALLY ENABLED  
IMAGING SYSTEM

Art Unit: 3737

Examiner: Ramirez, John Fernando

Confirmation No. 6101

**Electronically Filed on February 9, 2009**

**SECOND APPEAL BRIEF**

Mail Stop Appeal Brief – Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

The Applicant respectfully requests that the Board of Patent Appeals and Interferences reverse the final rejection of claims 1, 4-10, 13-14 and 16-19 and 21-23 of the present application. A Final Office Action was mailed August 19, 2008. The Applicants filed a response to the Final Office Action on October 7, 2008, within two months of the mailing date of the Final Office Action. An Advisory Action was mailed, however, on January 23, 2009 indicating that the period for reply expires on the mailing date of the Advisory Action or the date set forth in the Final Office Action, whichever is later. The Applicant respectfully requests a 1 month extension of time in which to respond. Thus, the period for reply ends on February 19, 2009 (six months from the mailing date of the Final Office Action). This Appeal Brief is being filed with a Notice of Appeal.

**REAL PARTY IN INTEREST  
(37 C.F.R. § 41.37(c)(1)(i))**

The real party in interest is G.E. Medical Systems Global Technology Co., assignee of the present application, having a place of business at 3000 North Grandview Boulevard, Waukesha, Wisconsin 53188.

**RELATED APPEALS AND INTERFERENCES  
(37 C.F.R. § 41.37(c)(1)(ii))**

Not Applicable.

**STATUS OF THE CLAIMS  
(37 C.F.R. § 41.37(c)(1)(iii))**

The present application includes pending claims 1, 4-10, 13-14 and 16-19 and 21-23, all of which remain rejected. Claims 2-3, 11-12, 15, 20 and 24-27 were canceled without prejudice or disclaimer.<sup>1</sup> The Applicant identifies claims 1, 4-10, 13-14 and 16-19 and 21-23 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

**STATUS OF AMENDMENTS  
(37 C.F.R. § 41.37(c)(1)(iv))**

Subsequent to the final rejection of the claims mailed August 19, 2008, the Applicant filed a Response Under 37 C.F.R. § 1.116.<sup>2</sup> The Response did not amend any of the pending claims.<sup>3</sup>

---

<sup>1</sup> See March 20, 2007 Amendment Under 37 C.F.R. § 1.116 and May 15, 2008 Amendment Under 37 C.F.R. § 1.111.

<sup>2</sup> See October 7, 2008 Response Under 37 C.F.R. § 1.116.

<sup>3</sup> See *id.*

**SUMMARY OF CLAIMED SUBJECT MATTER**  
**(37 C.F.R. § 41.37(c)(1)(v))**

**Independent claim 1 recites the following:**

An imaging system<sup>4</sup> comprising:

a central processing unit;<sup>5</sup>

a data storage unit in communication with said central processing unit;<sup>6</sup>

a medical imaging device in electrical communication with said central processing unit;<sup>7</sup>

and

a biometric authorization unit in electrical communication with said central processing unit,<sup>8</sup> wherein a user inputs a biometric identifier into said biometric authorization unit in order to enable imaging use of the medical imaging system,<sup>9</sup> wherein biometric data extracted from the biometric identifier is compared with stored biometric data in said data storage unit,<sup>10</sup> wherein the stored biometric data is associated with stored personal identification information,<sup>11</sup> wherein the stored biometric data and the stored personal identification information are stored after an initial registration,<sup>12</sup> and wherein user preference information with respect to imaging

---

<sup>4</sup> See *present application*, e.g., at page 3, lines 1-2, page 7, lines 4-22 and Figure 1, reference numeral 10.

<sup>5</sup> See *id.*, e.g., at page 3, lines 1-2, page 7, lines 4-10 and Figure 1, reference numeral 14.

<sup>6</sup> See *id.*, e.g., at page 3, lines 1-2, page 7, lines 4-10 and Figure 1, reference numeral 14.

<sup>7</sup> See *id.*, e.g., at page 3, lines 3-4, page 8, line 16 to page 12, line 14, Figure 3, reference numeral 11, Figure 4, reference numeral 42, Figure 5, reference numeral 84 and Figure 6, reference numeral 100.

<sup>8</sup> See *id.*, e.g., at page 3, lines 5-6, page 7, lines 5-8, page 8, lines 1-15, Figure 1, reference numeral 20, Figure 4, reference numeral 20 and Figure 5, reference numeral 82.

<sup>9</sup> See *id.*, e.g., at page 3, lines 6-8.

<sup>10</sup> See *id.*, e.g., at page 3, lines 8-10, page 8, lines 3-9 and page 14, lines 1-10.

<sup>11</sup> See *id.*, e.g., at page 3, lines 10-12 and page 14, lines 1-10.

<sup>12</sup> See *id.*, e.g., at page 12, lines 5-22, page 13, lines 1-11 and page 14, lines 11-21.

capabilities of said medical imaging device is associated with the stored biometric data and with the personal identification information.<sup>13</sup>

**Independent claim 10 recites the following:**

A medical imaging network<sup>14</sup> comprising a plurality of medical imaging systems<sup>15</sup> in communication with one another,<sup>16</sup> each of said medical imaging systems comprising:

a medical imaging device;<sup>17</sup> and

a biometric authorization unit,<sup>18</sup> wherein a user inputs a biometric identifier into said biometric authorization unit in order to use the medical imaging device to image a patient;<sup>19</sup> and

a central management station in communication with each of said plurality of medical imaging systems,<sup>20</sup> wherein biometric data extracted from the biometric identifier is stored in at least one of a central data storage unit in said central management station and individual data storage units in said plurality of imaging systems,<sup>21</sup> wherein personal identification information and user preference information with respect to imaging capabilities of said medical image device are associated with the stored biometric data.<sup>22</sup>

---

<sup>13</sup> See *id.*, e.g., at page 3, lines 12-14, page 13, lines 12-22 and page 14, lines 1-10.

<sup>14</sup> See *id.*, e.g., at Figure 5, reference numeral 72.

<sup>15</sup> See *id.*, e.g., at Figure 5, reference numeral 74.

<sup>16</sup> See *id.*, e.g., at page 4, lines 6-8, page 15, line 8 to page 16, line 12.

<sup>17</sup> See *id.*, e.g., at page 3, lines 3-4, page 8, line 16 to page 12, line 14, Figure 3, reference numeral 11, Figure 4, reference numeral 42, Figure 5, reference numeral 84 and Figure 6, reference numeral 100.

<sup>18</sup> See *id.*, e.g., at page 3, lines 5-6, page 7, lines 5-8, page 8, lines 1-15, Figure 1, reference numeral 20, Figure 4, reference numeral 20 and Figure 5, reference numeral 82.

<sup>19</sup> See *id.*, e.g., at page 3, lines 6-8.

<sup>20</sup> See *id.*, e.g., at page 4, lines 8-9, page 15, lines 8-20 and Figure 5, reference numeral 76.

<sup>23</sup> See *id.*, e.g., at page 4, lines 8-12, page 15, lines 8-20.

<sup>22</sup> See *id.*, e.g., at page 3, lines 12-14, page 12, lines 5-22, page 13, lines 12-22, page 13, lines 1-

**Independent claim 19** recites the following:

A method of using a medical imaging system<sup>23</sup> comprising:

registering to use the medical imaging system,<sup>24</sup> said registering comprising:

(i) inputting a biometric identifier into a biometric authorization unit;<sup>25</sup>

(ii) inputting personal information into the medical imaging system;<sup>26</sup> and

(iii) associating biometric data extracted from the biometric identifier with the personal information;<sup>27</sup>

storing the biometric data and associated personal information;<sup>28</sup>

storing individual imaging preferences for the medical imaging system as user preference information<sup>29</sup> and associating the user preference information with the biometric data and the personal information;<sup>30</sup> and

enabling imaging use of the medical imaging system when biometric data input at the biometric authorization unit matches stored biometric data.<sup>31</sup>

**Dependent claim 21** recites the following:

The method of claim 19, further comprising allowing said registering step by inputting a password.<sup>32</sup>

---

22 and page 14, lines 1-21.

<sup>23</sup> See *id.*, e.g., at page 4, lines 13-14.

<sup>24</sup> See *id.*, e.g., at page 4, lines 13-14.

<sup>25</sup> See *id.*, e.g., at page 4, lines 17-18 and Figure 7, reference numeral 122. .

<sup>26</sup> See *id.*, e.g., at page 4, lines 18-19 and Figure 7, reference numeral 124. .

<sup>27</sup> See *id.*, e.g., at page 4, lines 19-20 and Figure 7, reference numeral 126. .

<sup>28</sup> See *id.*, e.g., at page 4, lines 14-15.

<sup>29</sup> See *id.*, e.g., at page 3, lines 10-12 and page 14, lines 1-10.

<sup>30</sup> See *id.*, e.g., at page 3, lines 12-14, page 13, lines 12-22 and page 14, lines 1-10.

<sup>31</sup> See *id.*, e.g., at page 4, lines 15-17.

<sup>32</sup> See *id.*, e.g., at page 4, lines 20-21.

**GROUND OF REJECTION TO BE REVIEWED ON APPEAL**  
**(37 C.F.R. § 41.37(c)(1)(vi))**

- Claims 1, 4-6, 8, 14, 16, 18-19, 21 and 23 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. 6,129,671 (“Hastings”) in view of U.S. 2003/0088781 (“ShamRao”) and U.S. 5,315,999 (“Kinicki”).
- Claims 7, 9, 10, 13, 17 and 22 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hastings in view of ShamRao, Kinicki and U.S. 6,260,021 (“Wong”).

**ARGUMENT**  
**(37 C.F.R. § 41.37(c)(1)(vii))**

In order for a *prima facie* case of obviousness to be established, the Manual of Patent Examining Procedure (“MPEP”) states the following:

The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

See the MPEP at § 2142, citing *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), and *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval). Additionally, if a *prima facie* case of obviousness is not established, the Applicant is under no obligation to submit evidence of nonobviousness:

The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

See MPEP at § 2142.

The law and the MPEP are also clear that “[t]o establish *prima facie* obviousness of a claimed invention, **all the claim limitations** must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).” See MPEP at 2143.03 (emphasis added). Further, “[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art.” *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA).” See *id.*

As noted above, **Hastings, ShamRao and Kinicki** form the basis for all the claim rejections. However, none of the cited references describes, teaches or suggests associating imaging preference information with biometric data.

**I. The Proposed Combination Of Hastings, ShamRao And Kinicki Does Not Render Claims 1, 4-6, 8, 14, 16, 18-19, 21 And 23 Unpatentable**

Claim 1 recites, in part, “wherein **user preference information with respect to imaging capabilities of said medical imaging device is associated with the stored biometric data and with the personal identification information.**” Claim 10 recites, in part, “wherein personal identification information and **user preference information with respect to imaging capabilities of said medical imaging device are associated with the stored biometric data.**” Further, claim 19 recites, in part, “storing **individual imaging preferences for the medical imaging system as user preference information and associating the user preference information with the biometric data and the personal information.**” Thus, the claims are clear that imaging preference information and biometric data are not just merely stored. Instead, the imaging preference information is associated with the biometric data.

The Office Action acknowledges that “Hastings does not expressly teach the steps of inputting personal information into the system, associating biometric data extracted from the biometric identifier with the personal information, storing the biometric data and associated

personal information after initial registration, and associating preference information with the stored biometric data and with the personal identification number.” *See* August 19, 2008 Office Action at pages 2-3.

In an attempt to overcome the deficiencies of Hastings, the Office Action relies on ShamRao. *See id.* In particular, the Office Action states that “ShamRao teaches the steps of inputting personal information into the system, associating biometric data extracted from the biometric identifier with the personal information, storing the biometric data and associated personal information after initial registration, and **associating preference information with the stored biometric data** and with the personal identification number....” *See id.* at page 3 (emphasis added).

ShamRao does not, however, make up for all the deficiencies of Hastings. For example, as explained below, ShamRao does not describe, teach or suggest associating imaging preference information with stored biometric data.

ShamRao “relates to systems and methods for ensuring security and convenience using a computer readable card.” *See* ShamRao at [0002]. ShamRao discloses a “card” that “stores an encrypted biometric identity image of a user’s biometric scan to compare against a subsequent biometric scan.” *See id.* at [0009]. “The identity image is compared with the biometric scan when security is necessary during login, or during a transaction.” *See id.*

ShamRao discloses personalization data stored on the card:

The PUM card can contain data that uniquely identifies the user. For example, the personalization data can include personal profile information including name, login id, passwords, address, phone numbers, bank information, credit level etc., and consumer preference information such as preferred websites, stores, brand names, size of clothing, music, software, games[.] The data will also include biometric data **to authenticate the user.**



*See id.* at [0061] (emphasis added). Thus, ShamRao discloses that various personal information is stored on the PUM card. Further, the card may also store biometric data to authenticate the user. However, ShamRao does not describe, teach or suggest that preference information, in general, or imaging preference information, in particular, is associated with the biometric data. In ShamRao, a user enters the card, and authenticates use of the card through biometric data. Preference information is stored on the card, but is not necessarily associated with the biometric data.

There is nothing in ShamRao that describes teaches or suggests imaging preference information at all. More particularly, there is absolutely nothing in Hastings or ShamRao that describes, teaches or suggests **“user preference information with respect to imaging capabilities of said medical imaging device,”** in general. Further, in seeming contradiction to the statement in the Final Office Action, there is absolutely nothing in ShamRao that describes, teaches or suggests associating user preference information with respect to **imaging capabilities of a medical device with “stored biometric data and with the personal identification information.”**

The Office Action acknowledges that “Hastings and ShamRao do not appear to specifically disclose that the user preference information is with respect to imaging capabilities of the medical imaging device.” *See* August 19, 2008 Office Action at page 3. Thus, those two references cannot, by definition, disclose associating such user imaging preference information with stored biometric data by itself or with personal identification information.

---

To overcome these deficiencies, the Office Action relies on Kinicki. *See id.*

Kinicki indicates that “sets of imaging parameter values are saved as **preset** modes.” *See* Kinicki at Abstract (emphasis added). The “ultrasound imaging system stores a plurality of sets

of imaging parameter values, each set corresponding to a preset mode.” *See id.* at column 2, lines 54-56.

Kinicki does not describe, teach or suggest, however, that the system stores biometric data or associates the preset modes with biometric data. Instead, the preset modes are saved by a user who then “later **selects** one of the preset modes.” *See id.* at column 3, lines 25-30. There is nothing in Kinicki, nor Hastings or ShamRao, that describes, teaches or suggests that a user selects these presets modes through inputting biometric information. Instead, Kinicki is clear that the “user can select and deselect presets that are to appear on the touch panel 38 using the trackball 36 and the Enter key.” *See id.* at column 8, lines 54-57. The preset modes are stored on the computer and a user selects them via an interface. *See id.* at column 6, lines 40-43 (“Initially, the operator selects an exam type and preset mode and adjusts the imaging parameter values to obtain a desired image on the display screen 14.”). While a user may configure personal preset modes, there is nothing in Kinicki that discloses that such personal preset modes are ever associated with biometric data.

Kinicki does not describe, teach or suggest **associating** user preference information (with respect to **imaging capabilities of a medical device**) with “**stored biometric data**” by itself or “**with the personal identification information.**” As noted above, Hastings and ShamRao also do not describe, teach or suggest such limitations. Thus, because none of Hastings, ShamRao or Kinicki describes, teaches or suggests “**user preference information with respect to imaging capabilities of said medical imaging device [that] is associated with the stored biometric data and with the personal identification information,**” the combination of the three references, by definition, also cannot describe, teach or suggest the limitations, as recited in claim 1.

In sum, the Office Action acknowledges that “Hastings does not expressly teach the steps of inputting personal information into the system, associating biometric data extracted from the biometric identifier with the personal information, storing the biometric data and associated personal information after initial registration, and associating preference information with the stored biometric data and with the personal identification number.” *See* August 19, 2008 Office Action at pages 2-3. Next, ShamRao does not describe, teach or suggest associating imaging preference information with stored biometric data.

Further, the Office Action acknowledges that “Hastings and ShamRao do not appear to specifically disclose that the user preference information is with respect to imaging capabilities of the medical imaging device.” *See* August 19, 2008 Office Action at page 3. Consequently, Hastings and ShamRao cannot, **by definition**, disclose associating such user imaging preference information (which the Office Action acknowledges neither reference discloses) with stored biometric data by itself or with personal identification information.

Finally, as explained above, Kinicki does not describe, teach or suggest **associating** user preference information with respect **to imaging capabilities of a medical device with “stored biometric data and with the personal identification information.”** Thus, the combination of Hastings, ShamRao and Kinicki, alone or in combination with one another, does not (indeed, cannot) describe, teach or suggest these limitations.

For at least the reasons discussed above, the proposed combination of Hastings, ShamRao and Kinicki does not render claims 1, 4-6, 8 unpatentable.

---

Similarly, the proposed combination of references does not describe, teach or suggest “wherein personal identification information and **user preference information\_with respect to imaging capabilities of said medical imaging device are associated with the stored biometric**

**data,”** as recited in claim 10. Further, none of these references, alone or in combination with one another, describes, teaches or suggests a “method of using a medical imaging system comprising ... “storing **individual imaging preferences for the medical imaging system as user preference information** and **associating the user preference information with the biometric data and the personal information,**” as recited in claim 19.

Thus, for at least these reasons, the Applicant respectfully requests reconsideration of the rejection of claims 1, 10, 19, and the claims that depend therefrom. The Applicant respectfully submits that the proposed combination of references does not render the pending claims unpatentable.

**II. The Proposed Combination Of Hastings, ShamRao, Kinicki And Wong Does Not Render Claims 7, 9, 10, 13, 17 And 22 Unpatentable**

The Applicant also respectfully submits that the proposed combination of Hastings, ShamRao, Kinicki and Wong does not render claims 7, 9, 10, 13, 17 and 22 for at least the reasons discussed above.

**III. The Final Office Action Fails To Establish A *Prima Facie* Case Of Obviousness With Respect To Claim 21 For An Additional Reason**

Additionally, the Office Action has not shown where any of the references disclose “**allowing said registering step** by inputting a password,” as recited in claim 21. *See* August 19, 2008 Office Action. Indeed, the Office Action does not even address the language of claim 21. *See id.* Thus, for at least this reason, the Office Action has not established a prima facie case of obviousness with respect to claim 21. Indeed, claim 21 should be in condition for allowance.

#### IV. CONCLUSION

As discussed above, the Applicant respectfully submits that the pending claims are allowable in all respects. Therefore, the Board is respectfully requested to reverse the rejections of pending claims 1, 4-10, 13-14 and 16-19 and 21-23.

#### V. PAYMENT OF FEES

The Applicant previously paid \$500 for the first Notice of Appeal (*see* April 17, 2007 Notice of Appeal) and \$500 for the first Appeal Brief (*see* April 17, 2007 Appeal Brief). Thus, the Applicant only needs to pay the difference between the current fees for these Papers and those previously paid. The fee for the Notice of Appeal is now \$540, while the fee for the Appeal Brief is now \$540. Thus, the Applicant owes \$40 for the Second Notice of Appeal and \$40 for this Second Appeal Brief. The Commissioner is authorized to charge these fees (\$40 + \$40 = \$80), the **\$130 fee for the 1 month extension**, and any other necessary fees (or credit overpayment) to Deposit Account 07-0845.

Respectfully submitted,

Date: February 9, 2009

/Joseph M. Butscher/  
Joseph M. Butscher  
Registration No. 48,326

MCANDREWS, HELD & MALLOY, LTD.  
500 West Madison Street, 34th Floor  
Chicago, Illinois 60661  
Telephone: (312) 775-8000  
Facsimile: (312) 775-8100

**CLAIMS APPENDIX**  
**(37 C.F.R. § 41.37(c)(1)(viii))**

1. A medical imaging system comprising:

a central processing unit;

a data storage unit in communication with said central processing unit;

~~an~~ a medical imaging device in electrical communication with said central processing unit; and

a biometric authorization unit in electrical communication with said central processing unit, wherein a user inputs a biometric identifier into said biometric authorization unit in order to enable imaging use of the medical imaging system, wherein biometric data extracted from the biometric identifier is compared with stored biometric data in said data storage unit, wherein the stored biometric data is associated with stored personal identification information, wherein the stored biometric data and the stored personal identification information are stored after an initial registration, and wherein user preference information with respect to imaging capabilities of said medical imaging device is associated with the stored biometric data and with the personal identification information.

4. The medical imaging system of claim 1, wherein imaging use of the medical imaging system is allowed when a match exists between the biometric data extracted from the biometric identifier and the stored biometric data.

---

5. The medical imaging system of claim 1, wherein information regarding the use of the medical imaging system by the user is stored in said data storage unit.

6. The medical imaging system of claim 1, wherein said medical imaging device is an ultrasound probe and the medical imaging system is an ultrasound imaging system.

7. The medical imaging system of claim 1, wherein the medical imaging system is one of a Computed Tomography (CT), X-ray, Positron Emission Tomography (PET), Single Photon Emission Computed Tomography (SPECT), Electron Beam Tomography (EBT), Magnetic Resonance (MR), and image-guided surgery system.

8. The medical imaging system of claim 1, wherein the biometric identifier is at least one of a fingerprint, handprint, voice, iris, retina, and facial thermogram.

9. The medical imaging system of claim 1, wherein the medical imaging system is networked into at least one other imaging system.

10. A medical imaging network comprising a plurality of medical imaging systems in communication with one another, each of said medical imaging systems comprising:

a medical imaging device; and

a biometric authorization unit, wherein a user inputs a biometric identifier into said biometric authorization unit in order to use the medical imaging device to image a patient; and

a central management station in communication with each of said plurality of medical imaging systems, wherein biometric data extracted from the biometric identifier is stored in at least one of a central data storage unit in said central management station and individual data storage units in said plurality of imaging systems, wherein personal identification information

and user preference information with respect to imaging capabilities of said medical imaging device are associated with the stored biometric data.

13. The medical imaging network of claim 10, wherein use information, including at least one of user identity, time, and length of an imaging session at each of said plurality of imaging systems is stored within at least one of said central management station and any of said plurality of imaging systems.

14. The medical imaging network of claim 10, wherein a user initially registers at one of said central management station and one of said plurality of imaging systems.

16. The medical imaging network of claim 10, wherein at least one of said plurality of imaging devices is an ultrasound probe.

17. The medical imaging network of claim 10, wherein each of said plurality of imaging systems is one of a Computed Tomography (CT), X-ray, Positron Emission Tomography (PET), Single Photon Emission Computed Tomography (SPECT), Electron Beam Tomography (EBT), Magnetic Resonance (MR), and image-guided surgery system.

18. The medical imaging network of claim 10, wherein the biometric identifier is at least one of a fingerprint, handprint, voice, iris, retina, and facial thermogram.



19. A method of using a medical imaging system comprising:  
registering to use the medical imaging system, said registering comprising:

- (i) inputting a biometric identifier into a biometric authorization unit;
- (ii) inputting personal information into the medical imaging system; and
- (iii) associating biometric data extracted from the biometric identifier with the personal information;

storing the biometric data and associated personal information;

storing individual imaging preferences for the medical imaging system as user preference information and associating the user preference information with the biometric data and the personal information; and

enabling imaging use of the medical imaging system when biometric data input at the biometric authorization unit matches stored biometric data.

21. The method of claim 19, further comprising allowing said registering step by inputting a password.

22. The method of claim 19, wherein the medical imaging system is one of an ultrasound, Computed Tomography (CT), X-ray, Positron Emission Tomography (PET), Single Photon Emission Computed Tomography (SPECT), Electron Beam Tomography (EBT), Magnetic Resonance (MR), and image-guided surgery system.

23. The method of claim 19, wherein the biometric identifier is at least one of a fingerprint, handprint, voice, iris, retina, and facial thermogram.

**EVIDENCE APPENDIX**  
**(37 C.F.R. § 41.37(c)(1)(ix))**

- (1) United States Patent No. 6,129,671 (“Hastings”), entered into record in Office Action mailed February 21, 2007.
- (2) United States Patent Application Publication No.2003/0088781 (“ShamRao), entered into record in Office Action mailed April 15, 2008.
- (3) United States Patent No. 5,315,999 (“Kinicki”), entered into record in Office Action mailed February 21, 2007.
- (4) United States Patent No. 6,260,021 (“Wong”), entered into record in Office Action mailed February 21, 2007.

**RELATED PROCEEDINGS APPENDIX**  
**(37 C.F.R. § 41.37(c)(1)(x))**

Not Applicable.